UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

UNITED STATES OF AMERICA	**§**	
	§	
v.	**§**	**CRIMINAL NO.: 4:16-CR-00154-1**
	§	
CODY JACK WESTMORELAND	**§**	

MEMORANDUM IN SUPPORT OF MOTION TO SUPRESS EVIDENCE

TO THE HONORABLE JUDGE OF SAID COURT:

COMES NOW CODY JACK WESTMORELAND, the Defendant in the above styled and numbered cause and files this motion to suppress pursuant to Fed. R. Crim. P. 12(b)(3)(c) for an order suppressing all evidence obtained from the Government's deployment of a "Network Investigation Technique". Mr. Westmoreland also seeks suppression of the fruits of the Governments illegal search. Mr. Westmoreland has been charged with receipt and possession of child possession of child pornography, as well as, intent to view child pornography. Trial is scheduled for December 5, 2016.

II. Statement of Facts

On November 6, 2015, FBI agents executed a search warrant at the home of Cody Westmoreland which is shared with his girlfriend Pharrah McDonald in Houston, Texas. Mr. Westmoreland is 26 years old, with no criminal history, and was recently accepted to study engineering at the University of Texas, Austin. The search was conducted pursuant to a warrant issued by the Honorable John Froeschner.

The events leading to the search of Mr. Westmoreland's home began on February 20, 2015, when the government seized control of a "deep web" site described in the warrant application as

"Website A". "Website A" is run and administrated in Virginia. "Website A" is described as a "child pornography bulletin board and website dedicated to the advertisement and distribution of child pornography and the discussion of matter pertinent to the sexual abuse of children." Id. While there are illegal images hosted on "Website A" the site also contains legitimate content, including pictures, videos, and discussion forums (See Exhibit 1 & 2).

This site cannot be found on Google but is hosted on what has been called the "deep web". This name is given not to imply a sinister nature of the "deep web", but merely as a description. The websites found on the deep web cannot be found on Google or normal web browsers such as Chrome or Firefox. The "deep web" was developed by the United States Government to allows intelligence agents to communicate via the internet anonymously. The program created was called Tor or "the onion router". Now open to the public as free, downloadable software, Tor is used by people worried about their cyber security, freedom fighters in countries ruled by tyrants, and several other legal uses. Tor, like any tool, is used for legitimate purposes daily, but can be used for less savory purposes as well.

"Website A" was discovered by a foreign law enforcement agency, which provided the IP address to the FBI in December, 2014. The website was discovered during a "misconfiguration of the server" which allowed its IP address (normally undiscoverable) to be discovered and allowing investigators to collect information about the site. Following this investigation, the administrator of the site was arrested in February, 2015. Instead of dismantling the site or blocking the content from the public view, the FBI continued to run the site, unaltered for three months. During this three-month period the United States government was the largest distributor of child pornography in the world.

The FBI seized and ran the site in order to intercept electronic communications of the "target site's" private chat and messaging services between unknown "target subjects" or "unidentified administrators and users." In order to do this the FBI obtained authorization pursuant to 18 U.S.C. § 2518, commonly referred to as "Title III" or "the Wiretap Act". In this application the Government stated that in addition to the monitoring of chat and messages, it would deploy a "Network Investigative Technique" (NIT) that would work in the following way:

> The NIT will send one or more communications to TARGET SUBJECTS that access the TARGET WEBSITE after the date of its deployment, which communications are designed to cause the computer receiving it (sic) to deliver data that will help identify the computer, its location, other information about the computer, and the user of the computer accessing the TARGET WEBSITE. In particular, the NIT is designed to reveal to the government the computer's actual IP address… and other information that may assist in identifying computers that accesses (sic) the TARGET WEBSITE and their users.

It was also stated in the Wiretap application that the FBI would seek a separate warrant for the deployment of the NIT

The application for the warrant allowing the NIT to be used sought authorization to search any and all "activating computers," which are the computers "of any user or administrator who logs into the TARGET WEBSITE by entering a username and password." The warrant further stated that the NIT would be used to seize IP addresses, the type of operating systems on the computers, and whether the "NIT has already been delivered to the activating computer".

The application goes on to say that "in order to ensure technical feasibility and avoid detection of the technique by suspects under investigation" the NIT may be deployed against "any user who logs into the TARGET WEBSITE," regardless of the nature or extent of their activities in connection with the site. This means that users who were on the site for legitimate reasons had their computers infected with the FBI's NIT and their private information sent to the Government.

This is at issue due to the fact that the NIT application fails to allege that anyone who visited the TARGET WEBSITE necessarily viewed or downloaded illegal pictures. The application makes no claims that the name of the site identifies it as a source of child pornography or illegal activity. The website has several forums and chat discussion areas that do not hint at illegal or illicit materials, such as, "general discussion" and "security and technology".

Finally, the FBI requested authorization to delay providing notifications to the targets of the NIT search for a period of "30 days after any individual accessing the TARGET WEBSITE has been identified to a sufficient degree as to provide notice, unless the Court finds good cause for further delayed disclosure". While the court did grant this request it stipulated that notification must be given before the end of this thirty-day period, it appears no extension was granted to this time frame.

III. Argument

Given the facts so far presented it is clear that the Government's search of Mr. Westmoreland's computer, computer equipment, and home, were conducted in violation of Fed. R. Crim. P. 41. Rule 41 is a critical part of the rules of criminal procedure because it specifically strengthens and protects the 4th Amendment. When this rule has been violated by the Government the penalty is clear, suppression is the only appropriate remedy to counteract the Governments violation of Rule 41.

A. The Warrant Violated Rule 41

The searches of Mr. Westmoreland's home and computers were directly proceeded by the illegal infiltration of his private computer by the Government. The Government operated a website which contained both innocuous and illicit materials. They then collected data from each computer which visited the site through the NIT. They did not discriminate in the collection of

this data. Regardless of country, region, state, if you visited "Website A" your computer was infected with the NIT and your information was collected. This is a clear violation of Fed. R. Crim. P. 41.

Rule 41 specifies five different scenarios in which a magistrate judge may issue a warrant.

> (b) Authority to Issue a Warrant. At the request of the federal law enforcement officer or an attorney for the government:
>
> (1) a magistrate judge with authority in the district -- or if none is reasonably available, a judge of a state court of record in the district -- has authority to issue a warrant to search for and seize a person or property located within the district;
>
> (2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;
>
> (3) a magistrate judge--in an investigation of domestic terrorism or international terrorism--with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district;
>
> (4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; and
>
> (5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within any of the following:

> (A) a United States territory, possession, or commonwealth;
>
> (B) the premises--no matter who owns them--of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or
>
> (C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

The warrant issued in Mr. Westmoreland's case clearly does not fit into any of the above categories. Logic therefore dictates that the warrant was unlawfully issued. This District has previously agreed with this logic. In *In re Warrant to Search a Target Computer at Premises Unknown,* 958 F. Supp. 2d 753 (S.D. Tex. 2013) ("*In re Warrant")* the Government was involved with the investigation of fraud by unknown persons on an unknown computer. *Id* at 755. The Government sought a warrant that would allow them to "surreptitiously install data extraction software" on the unknown computer, in the unknown location. This software would allow the Government to extract identifying information from the computer. *Id.*

The Government in *In re Warrant* sought a warrant based on Rule 41(b)(1). *In re Warrant,* 958 F. Supp. 2d at 756. This rule subsection allows a magistrate judge to issue a warrant within a district. While the Government did cede the point that they did not know where the target computer was located, they continued under the theory that the "search" would not take place until the computer was located within the authorizing district. The court rejected the theory that a search of computer information is not conducted until a physical search of the computer has taken place. *Id*. Instead the courts ruled that a search takes place when the data of the computer is breached. *Id.* Due to this ruling the warrant allowing the use of the NIT from a district in Virginia must be ruled invalid because the data seized in this case was found during a search of a computer located in Houston, Texas.

1. The Warrant Would Be Invalid Under Any of the Other Subsection of Rule 41(b)

In re Warrant not only stated that the search of a computer in an unknown location was invalid, but had the foresight to rule that it is also invalid under Rule 41(b)(2). Rule 41(b)(2) states,

> a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;

In re Warrant dealt with this issue by stating,

> This subsection allows an extraterritorial search or seizure of moveable property "if it is located within the district when the warrant is issued but might move or be moved outside of the district before the warrant is executed." FED.R.CRIM.P. 41(b)(2) does not authorize a warrant in the converse situation --- that is, for property outside the district when the warrant is issued, but brought back inside the district before the warrant is executed. A moment's reflection reveals why this is so. If such warrants were allowed, there would effectively be no territorial limit for warrants involving personal property, because such property is moveable and can always be transported to the issuing district, regardless of where it might initially be found. *Id.* At 757.

Rule 41(b)(3) is also disqualified as this is not a case involving terrorism.

Rule 41(b)(4) deal with tracking devices. The Government has yet to set the precedent that a NIT should be treated as a tracking device. However, even if such precedent comes about Rule 41(b)(4) would still declare the warrant in this case to be invalid. This is due to the fact that *In re Warrant* states "this is not showing that the installation of the 'tracking device' (i.e. the software) would take place within this district. To the contrary, the software would be installed on a computer whose location could be anywhere on this planet." *Id* at 758. In this case the warrant allowing the use of the NIT was issued in Virginia, Mr. Westmoreland's computer was located in Houston, Texas, when the NIT infiltrated his computer and sent back the location data to the Government.

Rule 41(b)(5) would also not be applicable to this case. Rule 41(b)(5) allows for a "magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia" to approve a warrant for property located outside of that district. This provision is restricted to certain specified areas. These areas include United States territories or diplomatic missions.

B. Violation of Rule 41 Requires Suppression

It has been a long set precedent at every level of the criminal court system that when a warrant is defective the subsequent evidence produced as a result of that warrant is to be suppressed. The exact standard is as follows

> Suppression of evidence obtained through a search that violates Federal Rule of Criminal Procedure 41 is required only if: 1) the violation rises to a 'constitutional magnitude;' 2) the defendant was prejudiced, in the sense that the search would not have occurred or would not have been so abrasive if law enforcement had followed the Rule; 3) officers acted in 'intentional and deliberate disregard' of a provision in the Rule.

United States v. Weiland, 420 F.3d 1062, 1071 (9th Cir. 2005).

In this case it is clear that Mr. Westmoreland's 4th Amendment right against unreasonable search and seizure has been violated. Mr. Westmoreland had his computer virtually searched just because he visited a website. Furthermore, the warrant used in this case was invalid due to the restriction of the warrant to Virginia while Mr. Westmoreland and his computer were in Houston, Texas, when the search occurred.

The defect of this warrant is not merely administrative or clerical. There was not an obvious oversight such as a missing word or spelling defect, but a clear violation of the statute under which the warrant was sought.

The second prong was also violated during the search of Mr. Westmoreland's computer. If the Government had not disregarded the standards set out in Rule 41, the search would not have taken place. Mr. Westmoreland was not a suspect before the search of his computer took place. In all respects Mr. Westmoreland was simply unknown to the FBI or any law enforcement in regards to any criminal investigation. If not for the Government violating the terms of the warrant sought under Rule 41, Mr. Westmoreland would have never been identified nor his computer searched.

Finally, the third prong of the *United States v. Weiland* was also violated. *In re Warrant* was a known case at the time this warrant was issued. Furthermore, Rule 41 was easily accessible and understandable to anyone who could do a simple google search. The Government in this case clearly and deliberately over stepped their bounds with no regard for the rule of law.

C. The Government's Deliberate Violation of Rule 41's Notice Requirements Also Supports Suppression

If there can be any doubt that the third prong of *United States v. Weiland* was satisfied, then the blatant disregard of Rule 41(f)(1)(C) should show clear intent. Rule 41(f)(1)(c) states, "The officer executing the warrant must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken or leave a copy of the warrant and receipt at the place where the officer took the property." In this case Mr. Westmoreland was not provided with a copy of the warrant nor receipt for the data taken when the NIT was installed on his computer.

Rule 41(f)(3) does allow for the Government to delay notifying the target of the search if authorized by statute. The Government opted for this option and chose 18 U.S.C. § 3130a(b) as

their vehicle. 18 U.S.C. § 3130a(b), allow for delayed notice of a search of electronic information if the issuing court finds, that immediate disclosure would seriously jeopardize an investigation. However, this statute does not allow for notice to be suspended indefinitely. The Government was given thirty days to delay notice to those who had been searched through use of the NIT, but records received by this office show that no notice was ever given until defense council was provided with discovery. This is a willful and blatant act undertaken by the FBI. They directly ignored a condition of the warrant and demonstrated a complete lack of respect for the 4th Amendment.

III. Conclusion

Mr. Westmoreland is a law abiding citizen who visited a website. A website which was being staked out by the FBI, who would search your computer regardless of whether one was visiting for illicit or legitimate purposes. The FBI used a search warrant they knew or should of known would be invalid due to the fact that the computers they were searching were at unknown locations. The FBI used a warrant issued and constrained to the confines of Virginia to Search a computer in Houston, Texas. The FBI failed upon searching Mr. Westmoreland's computer to provide him with a copy of the warrant or notice of the search well beyond the thirty days in which they were given. Given these egregious sins against the 4th Amendment and previous rulings this court has an obligation to suppress all evidence recovered against Mr. Westmoreland as a result of the use of the NIT with the invalid warrant.

IV. Prayer

WHEREFORE, the Defendant prays that the Court all evidence obtained using the NIT and its fruits.

Respectfully submitted,

/s/ Timberly J. Davis
TIMBERLY J. DAVIS
SBN: 24040772
SDBN: 796518
2101 Crawford St, Suite 309
Houston, Texas 77002
Tel. (713) 224-7400
Fax. (713) 224-7402
timberly@tjdavislawfirm.com

CERTIFICATE OF SERVICE

I, TIMBERLY J. DAVIS, Attorney, certify that on the 14th day of October 2016, a copy of the foregoing Motion to suppress has been forwarded to the following counsel of record Assistant United States Attorney Kimberly Leo, and was contacted v*ia email* *Kim.Leo@usdoj.gov*, or, be ECF filing, or by fax via: (713) 718-3300 by my office about this motion in accordance with the District's service rules by e-mail about our intent to file these motions.

Respectfully submitted,

/s/ Timberly J. Davis_____
TIMBERLY J. DAVIS
SBN: 24040772
SDBN: 796518
2101 Crawford St, Suite 309
Houston, Texas 77002
Tel. (713) 224-7400
Fax. (713) 224-7402
timberly@tjdavislawfirm.com

ATTORNEY FOR
CODY WESTMORELAND

CERTIFICATE OF CONFERENCE

I, TIMBERLY J. DAVIS, Attorney, certify that on the 14th day of October 2016, a copy of the foregoing Motion to suppress has been forwarded to the following counsel of record Assistant United States Attorney Kimberly Leo, and was contacted v*ia email* *Kim.Leo@usdoj.gov*, or, be ECF filing, or by fax via: (713) 718-3300 by my office about this motion in accordance with the District's service rules by e-mail about our intent to file these motions.

Respectfully submitted,

/s/ Timberly J. Davis_____
TIMBERLY J. DAVIS
SBN: 24040772
SDBN: 796518
2101 Crawford St, Suite 309
Houston, Texas 77002
Tel. (713) 224-7400
Fax. (713) 224-7402
timberly@tjdavislawfirm.com

ATTORNEY FOR
CODY WESTMORELAND

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

UNITED STATES OF AMERICA	**§**	
	§	
v.	**§**	**CRIMINAL NO.: 4:16-CR-00154-1**
	§	
CODY JACK WESTMORELAND	**§**	

ORDER

On this day came on to be heard Defendant's Memorandum in Support of the Motion to suppress. The Court, having

considered the motion and argument of counsel, it is hereby _____.

SIGNED this ____ day of _____, 20___.

_____
JUDGE PRESIDING